IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

AMALGAMATED BANK, a New York banking corporation, individually and on behalf of a class of similarly situated financial institutions,

Plaintiff,

v.

HOME DEPOT U.S.A., Inc., a Delaware corporation,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

Related Case: 1:14-CV-02975

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff AMALGAMATED BANK, individually and on behalf of others similarly situated, by its undersigned attorneys, hereby files suit against Defendant HOME DEPOT U.S.A., INC. and alleges:

I. INTRODUCTION

1. Plaintiff Amalgamated Bank brings this Class Action Complaint against Home Depot U.S.A., Inc. ("Home Depot") on behalf of banks, credit unions, and other financial institutions that suffered injury as a result of a massive

security breach beginning in April or early May of 2014 and continuing through September 2014. This breach related to as-yet unidentified assailants accessing Home Depot's computer network and compromising among other information (1) store customers' names, addresses, phone numbers, email addresses, credit and debit card numbers, card expiration dates, and card verification values ("CVVs") and (2) the states and ZIP codes of the stores associated with individual card transactions (the "Home Depot Data Breach").

2. The security breach likely includes the point-of-sale network that processes credit and debit card transactions for most, if not all, Home Depot retail stores in the United States, compromising the sensitive financial information of at least 56 million Home Depot customers.

3. The breach related to the assailants deploying commonplace malicious software ("malware") to collect customers' personal and financial information, as well as the states and ZIP codes of the stores associated with each card transaction. Hackers began using the malware to steal customer information which was then offered for sale on "rescator.cc.," an underground website known for trafficking in stolen card information. The attack compromised information for hundreds of thousands, if not millions, of customers, likely making it one of the largest data breaches ever recorded.

4. As a result of Home Depot's negligent security protocols, Home Depot not only enabled the theft of its customers' personal and financial information, as well as subsequent fraudulent charges on their debit and credit cards, but also did not even become aware of a potential security breach until September 2, 2014—five months after the breach began. This security failure by Home Depot is even more egregious in light of recent, high-profile security breaches at other major retailers including Target and Neiman Marcus. Customer information was therefore available for sale for at least five months.

5. Approximately one week after discovering the massive breach, Home Depot finally acknowledged on or about September 8, 2014 that the breach had occurred and that millions of customers' personal and financial information had been compromised.

6. Worse still, even after learning of the breach as it pertained to certain personal and financial information, on or about November 6, 2014, Home Depot announced that approximately 53 million customer email addresses had also been compromised.

7. As a direct result of Home Depot's negligent security practices, Plaintiff and the other financial institutions making up the proposed Class have incurred costs, and will incur future costs, totaling hundreds of millions of dollars.

Such costs have and will include: (1) reissuing debit and credit cards, (2) loss of customers, (3) covering the costs of fraudulent charges, (4) notifying customers of the breach, and (4) handling customer service inquiries and investigations related to the breach.

8. Fraudulent charges stemming from the breach are estimated to be between two and three billion dollars at this time, with an average of $332 in fraudulent charges on each stolen card.[1] That total is in addition to fraudulent charges stemming from "phishing scams, which are designed to trick customers into providing personal information in response to phony e-mails[.]"[2]

9. Accordingly, Plaintiff, individually and on behalf of the proposed Class, asserts claims against Home Depot for negligence, negligence *per se*, and negligent misrepresentation by omission.

II. PARTIES, JURISDICTION, AND VENUE

10. This is a class action for damages that exceed $5,000,000, exclusive of interest and costs.

[1] Mitch Lipka, "Home Depot Hack Could Lead to $3 Billion in Fake Charges." CBS (Sept. 16, 2014) (*available at* http://www.cbsnews.com/news/credit-

[2] Nick Turner, "Home Depot Says 53 Million E-Mail Addresses Taken in Breach." Bloomberg (Nov. 7, 2014) (*available at* http://www.bloomberg.com/news/2014-11-06/home-depot-says-53-million-e-mail-addresses-were-taken-in-breach.html).

11. Plaintiff Amalgamated Bank is a New York banking corporation and has its principal place of business at 275 7th Avenue, New York, NY 10001.

12. Defendant Home Depot U.S.A., Inc. is a Delaware corporation with its principal place of business located in Atlanta, Georgia. Home Depot is the world's largest home improvement retailer, selling a variety of tools, home goods, and construction supplies in its more than 2200 United States retail stores.

13. This Court has jurisdiction pursuant to and 28 U.S.C. § 1332(d)(2) (diversity of citizenship under the Class Action Fairness Act).

14. This Court has personal jurisdiction over Home Depot because Home Depot maintains its principal place of business in Georgia, regularly conducts business in Georgia, and has sufficient minimum contacts in Georgia. Home Depot intentionally avails itself of this jurisdiction by marketing and selling products from its principal place of business in Georgia to millions of customers across the United States, including in Georgia.

15. Venue is proper within this District because a substantial part of the events giving rise to the claims occurred in this District.

III. FACTUAL ALLEGATIONS

A. *Home Depot Failed to Meet Industry Regulations and Implement Appropriate Security Protocols for its Customers' Data*

16. Home Depot has been listed as the fifth largest retailer in the United States behind only Walmart, Kroger, Costco, and Target.[3] It has millions of customers across the United States.

17. Like most retailers, Home Depot processes debit and credit card payments for customer purchases in-store.

18. To process credit and debit transactions, Home Depot and other retailers contract with a bank. These contracts provide Home Depot and other merchants the ability to process credit and debit transactions.

19. When consumers make purchases at Home Depot, the relevant Home Depot location requests authorization for the transaction from the issuer (like Plaintiff or the other Class members) of the debit or credit card. If the issuing bank authorizes the transaction, Home Depot (through its merchant processor or settlement agent) processes the transaction and transmits said transaction to its processing/settlement bank with which Home Depot has contracted. The processing/settlement bank will credit Home Depot's account for the purchase, forwarding the final transaction to the issuing bank, at which point the issuing bank settles with the settlement/processing bank. Upon completion of this process, the

[3] National Retail Federation, "Top 100 Retailers Chart 2014." (*available at* https://nrf.com/2014/top100-table).

issuing bank will post the purchase charge to the customer's debit or credit card account.

20. Process payment networks, like Visa and Mastercard, often issue regulations ("Card Operating Regulations") binding on Home Depot and other retailers as a condition of their contract with a bank. The Card Operating Regulations mandate that Home Depot cannot disclose cardholder account numbers, personal information, magnetic stripe information, or transaction information to third parties other than the merchant's agent, the bank with which Home Depot contracted, or that bank's agents. Under the Card Operating Regulations, Home Depot was required to maintain the security and confidentiality of customer debit and credit card information and magnetic stripe information and protect that information from unauthorized disclosure.

21. Home Depot did not comply with the Card Operating Regulations and did not inform Plaintiff and the Class of its failure.

22. Home Depot was also required at the time of the breach to adhere to the Payment Card Industry Data Security Standard ("PCI DSS"). The PCI DSS are industry-wide standards that govern the security of financial information transmitted by debit and credit card purchases. On information and belief, Home Depot was required to adhere to comply with PCI DSS because of its contracts

with banks. At the time of the breach, PCI DSS 2.0 was in effect, and Home Depot held itself out as being compliant with all current standards for PCI DSS at the time of the breach.

23. PCI DSS generally represent only the most minimal precautions that a merchant like Home Depot should take to safeguard its customers' data.

24. PCI DSS requires merchants to: (a) secure properly personal information stored on debit and credit cards, (b) dispose of or destroy information contained on debit or credit cards after the time period necessary to authorize the transaction has passed, (c) keep the information contained on debit and credit cards from third parties by not disclosing such information or allowing it to be disclosed, and (d) track and monitor access to network resources and cardholder data. Home Depot did not adhere to any of these standards or inform Plaintiff and the Class of its failure to do so.

25. Home Depot should have implemented a security system to protect sensitive customer information under the relevant PCI DSS, including but not limited to installation of a firewall to prevent external access to its computer systems and other physical and electronic barriers to customer data. Home Depot did not adhere to any of these standards or inform Plaintiff and the Class of its failure to do so.

26. Under PCI DSS, Home Depot was also required to: (1) restrict physical and electronic access to its computer systems to only individuals who needed access for valid purposes, (2) create passwords, (3) use encryptions, and (4) assign unique IDs to each individual with access to its systems. Home Depot did not adhere to any of these standards or inform Plaintiff and the Class of its failure to do so.

27. Home Depot was also to monitor access to its computer networks and to cardholder account data on its systems to ensure that breaches would be detected and handled quickly, including conducting regular tests to ensure security protocols were operating properly and regularly reviewing lots for all system components. Home Depot did not adhere to any of these standards or inform Plaintiff and the Class of its failure to do so.

28. PCI DSS required Home Depot to dispose of or destroy information contained on debit or credit cards after the time period necessary to authorize the transaction has passed. Home Depot did not adhere to any of these standards or inform Plaintiff and the Class of its failure to do so.

29. At all relevant times, Home Depot was aware of its obligation to protect its customers' personal and financial data. Home Depot's participation in payment card processing networks put it on notice that its customers and the

financial institutions that issue cards to them relied on Home Depot to protect customers' personal and financial data from unauthorized access.

30. At all relevant times, Home Depot was aware that should it fail to protect its customers' personal and financial data, the financial institutions that issued cards to its customers would be injured, including but not limited to having to spend substantial resources to notify their customers, open and close cardholder accounts, reissue debit and credit cards, lose interest and transaction fees, monitor and prevent additional fraud, and reimburse cardholders for fraudulent transactions.

31. Information obtained by investigative journalists, security experts, government investigators, and by members of the United States Senate in hearings shows that the data breach could easily have been prevented, as Home Depot failed to take adequate and reasonable precautions to ensure its data systems were protected, ignored *clear* warnings that intruders had breached its systems, and failed to take actions that could have thwarted the breach.

32. Through its actions and inactions, Home Depot has violated statutory and common laws designed to prevent such disasters, and those violations have caused Plaintiffs and Class members to suffer substantial damages.

33. Home Depot has conceded that "[i]f we re[woun]d the tape, our security systems could have been better, as its former chief executive officer, Frank Blake, told the Wall Street Journal. According to Blake, "**data security just wasn't high enough in our mission statement**."[4]

34. Two former managers have also come forward and asserted that Home Depot's former information security chief, Jeff Mitchell, told them to use "C level security" because upgrading Home Depot's infrastructure would be expensive and could disrupt business systems. Over the last three years, dozens of employees have fled Home Depot's already small information security department, apparently frustrated with the protocols and lack of resources.[5] Employees were reportedly told "We sell hammers" when they requested more security training and equipment.[6]

---

[4] Shelly Banjo, "Home Depot Hackers Exposed 53 Million Email Addresses." Wall Street Journal Online (Nov. 6, 2014) (*available at* http://online.wsj.com/news/article_email/home-depot-hackers-used-password-stolen-from-vendor-1415309282-lMyQjAxMTA0NzAzNzMwMjc5Wj).

[5] Julie Creswell and Nicole Perlroth, "Ex-Employees Say Home Depot Left Data Vulnerable." The New York Times (Sept. 20, 2014) (*available at* http://www.nytimes.com/2014/09/20/business/ex-employees-say-home-depot-left-data-vulnerable.html?_r=0).

[6] Ben Elgin, Michael Riley, and Dune Lawrence, "Former Home Depot Managers Depict 'C-Level Security Before the Hack." Businessweek (Sept. 12, 2014)

B. *Home Depot Discovers its Security Was Breached Five Months after the Breach Started*

35. Home Depot asserts that it was not aware of a breach to its computer systems until law enforcement and Class members so notified it on or about September 2, 2014.

36. That same day, a large amount of debit and credit card information appeared for sale on "rescator.cc." a website known for trafficking in stolen financial information and perhaps best known for selling financial information gleaned from the highly-publicized cyber-attack on Target in 2013. Multiple banks asserted that Home Depot was likely the source of the stolen information and ample evidence confirmed those assertions. For example, security blogger Brian Krebs posted information showing that the ZIP code data of the newly-posted financial information overlapped with the ZIP code data from Home Depot stores 99.4 percent.[7]

37. Home Depot began to investigate the breach in September of 2014 along with the U.S. Secret Service and outside security firms. On September 8, 2014, Home Depot confirmed that its customers' personal and financial

---

(*available at* http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say).

[7] *See* http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/

information was compromised by the breach and that potential victims included anyone who used a debit or credit card in any of its over 2200 stores in the United States or Canada beginning in April of 2014.

38. Upon information and belief, Home Depot used weak password configurations and did not use lockout security procedures at remote access points, enabling hackers to gain access to its corporate IT network.

39. Once into Home Depot's networks, the hackers were able to use "RAM scraper" malware to gain access to Home Depot's customers' personal and financial information.

40. Home Depot did not detect the installation of RAM scraping malware on its point-of-sale terminals and did not take steps to eliminate such malware.

41. The RAM scraping malware enabled the hackers to steal customers' personal and financial information and move it to external servers the hackers controlled.

42. Home Depot was, or should have been, aware that RAM scraping malware poses a significant threat to retailers and customer information. Visa issued a Data Security Alert regarding the threat in 2009 instructing companies like Home Depot to "secure remote access connectivity," "implement secure network configuration, including egress and ingress filtering to only allow the ports/services

necessary to conduct business" (*i.e.*, segregate networks), "actively monitor logs of network components, including intrusion detection systems and firewalls for suspicious traffic, particularly outbound traffic to unknown addresses," "encrypt cardholder data anywhere it is being stored and [] implement[] a data field encryption solution to directly address cardholder data in transit," and "work with your payment application vendor to ensure security controls are in place to prevent unauthorized modification to the payment application configuration."[8]

43. It has been reported by both the media and private security companies that the Home Depot breach could affect over sixty million credit card accounts, twenty million more than were affected by the large-scale Target breach in 2013.[9]

44. At no time did Home Depot notify Plaintiff, or any Class members, about its deficient security systems. Plaintiff and Class members reasonably expected that Home Depot would safeguard confidential customer personal and financial information, particularly in light of several recent highly-publicized security breaches.

---

[8] *See* https://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf.

[9] Nicole Perlroth, "Home Depot Data Breach Could Be the Largest Yet." New York Times Blogs (Sept. 8, 2014) (*available* at http://bits.blogs.nytimes.com/2014/09/08/home-depot-confirms-that-it-was-hacked/).

45. Even though the breach occurred over a span of approximately five months, Home Depot was not even the first to discover or report the security breach.

C. *Home Depot Discovers Approximately 53 Million Customer Email Addresses Have Also Been Compromised*

46. On November 6, 2014, Home Depot announced that the breach was worse than it had originally anticipated and included not only the approximately 56 million debit and credit card accounts originally identified but also approximately 53 million email addresses that could be used to deceive customers into providing further sensitive personal and/or financial information through "phishing" scams.[10]

47. Despite being on notice that it had been the subject of one of the largest security breaches in the history of United States retailers, it took Home Depot yet another month to determine that these email addresses had also been compromised.

D. *Plaintiff and Class Members Were Damaged by Home Depot's Failure to Secure Sensitive Customer Personal and Financial Information Adequately*

[10] Shelly Banjo, "Home Depot Hackers Exposed 53 Million Email Addresses." Wall Street Journal Online (Nov. 6, 2014) (*available at* http://online.wsj.com/news/article_email/home-depot-hackers-used-password-stolen-from-vendor-1415309282-lMyQjAxMTA0NzAzNzMwMjc5Wj).

48. As a result of the massive data breach, Plaintiff and Class members have incurred significant monetary losses in connection with, among other things, cancelling and reissuing credit cards to their customers, notifying customers, closing and opening accounts, lost interest and transaction fees, lost customers, reimbursing customers for fraudulent transactions, and monitoring and preventing further fraud.

49. Home Depot did not adhere to basic industry standards nor did it effectively monitor its security systems to protect its customers' information. Home Depot's substandard, "C level security," improper retention of cardholder data, and failure to monitor its systems adequately for unauthorized access led to Home Depot's customers' personal and financial data being compromised for nearly half a year before other entities notified Home Depot of the breach. At no point during that nearly half year did Home Depot provide any warning to Plaintiff or Class members of the risks its lax security system posed to customers.

50. Home Depot could have prevented the security breach.

51. At the very least, Home Depot should have become aware of a potential breach in or about July of 2014 when Symantec employees conducted a "health check" on Home Depot's information security system and notified Home

Depot that it was using out-of-date malware detection systems. Hackers could have been accessing customers' personal and financial data at this point.[11]

52. Home Depot was also reportedly using out-of-date antivirus software for its point-of-sale systems, Symantec's Endpoint Protection 11, according to several former information security managers. Endpoint Protection 11 was released in 2007. Symantec's version 12, released in 2011, was touted by the company as protecting against the "explosion in malware scope and complexity" as the "threat landscape has changed significantly."[12] The same former information security managers reportedly pled with Home Depot to upgrade the severely outdated software.[13]

53. Home Depot knew, or should have known, that it was also to delete all cardholder data and prevent such data from being accessed by third parties.

54. Home Depot knew, or should have known, that it was required to monitor its system regularly to protect the safety of sensitive customer data.

55. Home Depot owed a duty to Plaintiff and the Class to comply with Card Operating Regulations, secure customers' personal and financial information,

[11] http://www.businessweek.com/articles/2014-09-12/home-depot-didnt-encrypt-credit-card-data-former-workers-say.

[12] *Id.*

[13] *Id.*

destroy or otherwise dispose of cardholder information after the time period necessary to process transactions, and prevent such information from being disclosed to third parties.

56. Home Depot breached each of these duties and negligently allowed sensitive cardholder data to be compromised and then sold.

57. As a result of the data breach, Plaintiff and Class members were damaged and required to spend, on an ongoing basis, substantial resources to notify customers, open and close cardholder accounts, reissue debit and credit cards, lose interest and transaction fees, monitor and prevent additional fraud, and reimburse customers for fraudulent transactions.

IV. CLASS ACTION ALLEGATIONS

58. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 57.

59. Pursuant to Federal Rule of Procedure 23(b)(2) and (3), Plaintiff brings this action on its own behalf and on behalf of a class of all persons similarly situated and defined as follows (collectively referred to as "the Class" or "Class"):

> All financial institutions—including, but not limited to, banks, and credit unions—in the United States (including its territories and the District of Columbia) that issue payment cards, including credit and debit cards, or perform, facilitate, or support card issuing services, whose customers made purchases from Home Depot

> stores during the period from April 1, 2014 to the present.[14]
>
> Excluded from the Class are Defendant and its parents, subsidiaries, and affiliates, any entity in which Defendant has a controlling interest, any officers or directors thereof, together with the legal representatives, heirs, successors, or assigns of any Defendant, and any judicial officer assigned to this matter and his or her immediate family.

60. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

61. This action has been brought and may properly be maintained as a class action as it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements. Plaintiffs seek to represent an ascertainable Class with a well-defined community of interest in the questions of law and fact involved in this matter.

62. Although the precise number of Class members is unknown and can only be determined through appropriate discovery, Plaintiffs believe and, on that basis, allege that the proposed class is so numerous that joinder of all members would be impracticable. The number of separate individuals whose private personal and financial data has been compromised as a result of the data breach

[14] Plaintiffs reserve the right to amend the Class definition as new details emerge regarding whether and when the breach has ended.

described herein is over 56 million. The number of financial institutions affected by the breach—all of whom are members of the proposed Class—total at least one thousand such that the number of individual plaintiffs would make joinder impossible.

63. Questions of law and fact common to the Plaintiff Class exist that predominate over questions affecting only individual members, including *inter alia*:

a) Whether Defendant owed a duty to Plaintiff and the Class members to protect cardholder personal and financial data;

b) Whether Defendant failed to provide adequate security to protect consumer cardholder personal and financial data;

(c) Whether Defendant negligently or otherwise improperly allowed cardholder personal and financial data to be accessed by third parties;

(d) Whether Defendant failed to notify adequately Plaintiff and Class members that its data system was breached;

(e) Whether Defendant negligently misrepresented that it would abide by industry standards and regulations to protect cardholder data;

(f) Whether Plaintiff and Class members suffered financial injury;

(g) Whether Defendant's failure to provide adequate security proximately caused Plaintiff and Class members' injuries;

(h) Whether Plaintiff and Class members are entitled to damages and, if so, the measure of such damages; and

(i) Whether Plaintiff and Class members are entitled to injunctive relief.

64. Plaintiffs are members of the putative Class. The claims asserted by the Plaintiffs in this action are typical of the claims of the members of the putative Class, as the claims arise from the same course of conduct by Defendant and the relief sought is common. Plaintiff and Class members' injuries, in the form of losses incurred as a result of, *inter alia*, reissuing debit cards and refunding fraudulent charges for accounts affected by the Home Depot Data Breach, as well as costs incurred in notifying customers of the Home Depot Data Breach, are the result of the same misconduct by Defendant alleged herein and Plaintiff and Class members assert the same claims for relief.

65. Plaintiff will fairly and adequately represent and protect the interests of the members of the putative Class, as their interests are coincident with, not antagonistic to, the other Class members'. Plaintiff has retained counsel competent and experienced in both consumer protection and class action litigation.

66. Certification of the Class is appropriate pursuant to Federal Rule of Civil Procedure 23(b)(2) and (3) because Defendant has acted with respect to the Class in a manner generally applicable to each Class member, there is a well-defined community of interest in the questions of law and fact involved in the action, which affect all class members, and questions of law or fact common to the respective members of the Class predominate over questions of law or fact affecting only individual members. This predominance makes class litigation superior to any other method available for the fair and efficient adjudication of these claims including consistency of adjudications. Absent a class action, it would be highly unlikely that the members of the Class would be able to protect their own interests because the cost of litigation through individual lawsuits might exceed the expected recovery.

67. A class action is an appropriate method for the adjudication of the controversy in that it will permit a large number of claims to be resolved in a single forum simultaneously, efficiently, and without the unnecessary hardship that would result from the prosecution of numerous individual actions and the duplication of discovery, effort, expense, and the burden on the courts that individual actions would create.

68. The benefits of proceeding as a class action, including providing a method for obtaining redress for claims that would not be practical to pursue individually, outweigh any difficulties that might be argued with regard to the management of the class action.

COUNT I – NEGLIGENCE

69. Plaintiff re-alleges and reaffirms herein all of the allegations contained in paragraphs 1 through 68.

70. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining and processing Plaintiff's customers' personal and financial information.

71. Defendant owed a duty to Plaintiff and the Class to provide adequate security to protect their mutual customers' personal and financial information.

72. Defendant breached its duties by (1) unreasonably allowing an unauthorized third-party intrusion of its computer systems; (2) failing to protect reasonably against such an intrusion; (3) unreasonably allowing third parties to access the private personal and financial information of its customers; and (4) failing to monitor appropriately its systems to detected unauthorized access, including but not limited to, failing to detect the intrusion for a period of four or more months.

73. Defendant knew or should have known of the PCI DSS industry standard and other relevant requirements regarding cardholder data security, as well as the attendant risks of retaining personal and financial data and the importance of providing adequate security.

74. Defendant knew or should have known of the risk that its point-of-service terminals could be attacked using methods similar or identical to those previously used against major retailers in recent months and years.

75. As a direct and proximate result of Home Depot's careless and negligent conduct, Plaintiff and the Class have suffered substantial financial losses as detailed herein.

76. These financial losses are increasing as additional fraudulent charges are discovered and with the recent revelation that customer email addresses were also compromised.

COUNT II – NEGLIGENCE *PER SE*

77. Plaintiff re-alleges and reaffirms herein all of the allegations contained in paragraphs 1 through 68.

78. Under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, Home Depot has a duty to protect and keep sensitive personal information that it obtained from

cardholders conducting debit and credit card transitions in its stores secure, private, and confidential.

79. Home Depot violated the Gramm-Leach-Bliley Act by: (1) failing to adequately protect its customers' sensitive personal and financial data and (2) failing to monitor and ensure compliance with the PCI DSS, as well as its contractual obligations and accompanying rules and regulations.

80. Home Depot's violation of the PCI DSS, as well as its contractual obligations and accompanying rules and regulations, constitutes negligence *per se*.

81. As a direct and proximate result of Home Depot's negligence *per se*, Plaintiff and the Class have suffered substantial financial losses as detailed herein.

COUNT III – NEGLIGENT MISREPRESENTATION BY OMISSION

82. Plaintiff re-alleges and reaffirms herein all of the allegations contained in paragraphs 1 through 68.

83. Home Depot, through its participation in the debit and credit card processing network, was required to comply with industry standards for card operation, including PCI DSS. To comply with such standards, Home Depot was required to protect adequately cardholder personal and financial data, monitor access to that data, and not to retain, store or disclose information obtained from card magnetic stripes beyond authorized boundaries.

84. Home Depot knew, or should have known, that it was not complying with PCI DSS and industry card operating regulations for protecting consumer data. Home Depot knew, or should have known, that it was not properly protecting cardholder personal and financial data.

85. Home Depot failed to communicate material information to Plaintiff and the Class regarding its lack of compliance with PCI DSS and Card Operating Regulations, including but not limited to the fact that it was not properly safeguarding cardholder personal and financial account data.

86. Home Depot's failure to inform Plaintiff and Class members of its non-compliance with PCI DSS and Card Operating Regulations was a material omission that should have been disclosed to Plaintiff and Class members.

87. Had Home Depot informed Plaintiff and Class members of its non-compliance with PCI DSS and industry regulations, Plaintiff and the Class would have been better able to protect themselves from the damages they have incurred and continue to incur.

88. As a direct and proximate result of Home Depot's negligent and improper conduct, Plaintiff and the Class have suffered substantial financial losses as detailed herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Amalgamated Bank, individually and on behalf of all others similarly situated, requests that the Court enter judgment against Defendant and in favor of Plaintiff and the Class and award the following relief:

A. Certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiff as representative of the Class and Plaintiff's counsel as counsel for the Class;

B. Injunctive relief enjoining Defendant from improperly retaining any customer personal or financial data;

C. Declaring that Defendant is financially responsible for notifying all Class members about the misconduct described herein;

D. Awarding Plaintiff and the Class actual damages, consequential damages, specific performance, restitution, and/or rescission, where appropriate;

E. Awarding Plaintiff and the Class pre- and post-judgment interest;

F. Awarding Plaintiff and the Class reasonable attorneys' fees and costs of suit; and

G. Awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all matters triable as of right by a jury.

November 13, 2014.

Respectfully submitted,

/s/ *Ranse M. Partin*
Ranse M. Partin **GA Bar No. 556260**
CONLEY GRIGGS PARTIN LLP
1380 West Paces Ferry Road, N.W.
Suite 2100
Atlanta, GA 30327
Telephone: (404) 467-1155
Facsimile: (404) 467-1166
Ranse@conleygriggs.com

Andrew N. Friedman, *pro hac pending*
Matthew S. Axelrod, *pro hac pending*
Douglas J. McNamara, *pro hac pending*
Sally M. Handmaker, *pro hac pending*
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW
East Tower, 5th Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699

Attorneys for Plaintiff Amalgamated Bank

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 7.1(D) of the Local Rules of the Northern District of Georgia, the undersigned hereby certifies that the foregoing was prepared in a font and point selection approved by this Court and authorized by Local Rule 5.1(B).

/s/ *Ranse M. Partin*
Ranse M. Partin
Georgia Bar **No. 556260**
ranse@conleygriggs.com
Conley Griggs Partin LLP
The Hardin Building
1380 West Paces Ferry Road, N.W., Suite 2100
Atlanta, Georgia 30327
(404) 467-1155: Office
(404) 467-1166: Fax